



# CMS HIPAA TRANSITION WORKSHOP

---

*Just When You Thought You Were  
Getting Close....*

Susan Fox, CMS A-Team/FOX Systems



# The Panelists

---

- Susan Fox,  
Moderator
- Judy Gelein, State of  
California
- Julie Dittman, State  
of California
- Leah Hole-Curry,  
A-Team/FOX
- Peter Barry, Peter T  
Barry Co.
- Mark Charles, State  
of Michigan
- Robin Pratt,  
A-Team/FOX



# Concept

---

- Present principles distilled from a two-day CMS workshop
- Encourage sharing of the pain and solutions
- Focus on final stage of preparation for the transition to compliant standards



# Readiness and Transition

---

- Readiness is a phase within the HIPAA master work plan that begins when assessment is done and remediation strategies are under way. It includes issue resolution, testing, strategic decisions, and partner agreements.
- Transition begins when the MMIS starts accepting live HIPAA transactions and ends when all HIPAA required transactions are cut-over to compliant processing.



# Topics

---

- Readiness (first hour):
  - Implementation Organizational Structure
  - Readiness and Contingency Plans
  - Readiness Issue Resolution
  - Trading Partner Agreements
- Testing (second hour):
  - Compliance Certification
  - Business to Business
  - Applications/Operations
- Transition (third hour):
  - Transition Plan
  - Sequencing Issues
  - Twisted Sisters



# Format

---

- Each panelist will introduce a topic and then will facilitate audience participation on the subject
- 1:30—2:30: Readiness Issues
- There will be a break at 2:30 -- 3:00
- 3:00—4:00: Testing
- 4:00—5:00: Transition Issues

# ORGANIZATIONAL STRUCTURE FOR IMPLEMENTATION



---

*What's good for the goose (assessment)  
may not be good for the gander  
(implementation)*

Judy Gelein and Julie Dittman, State of California



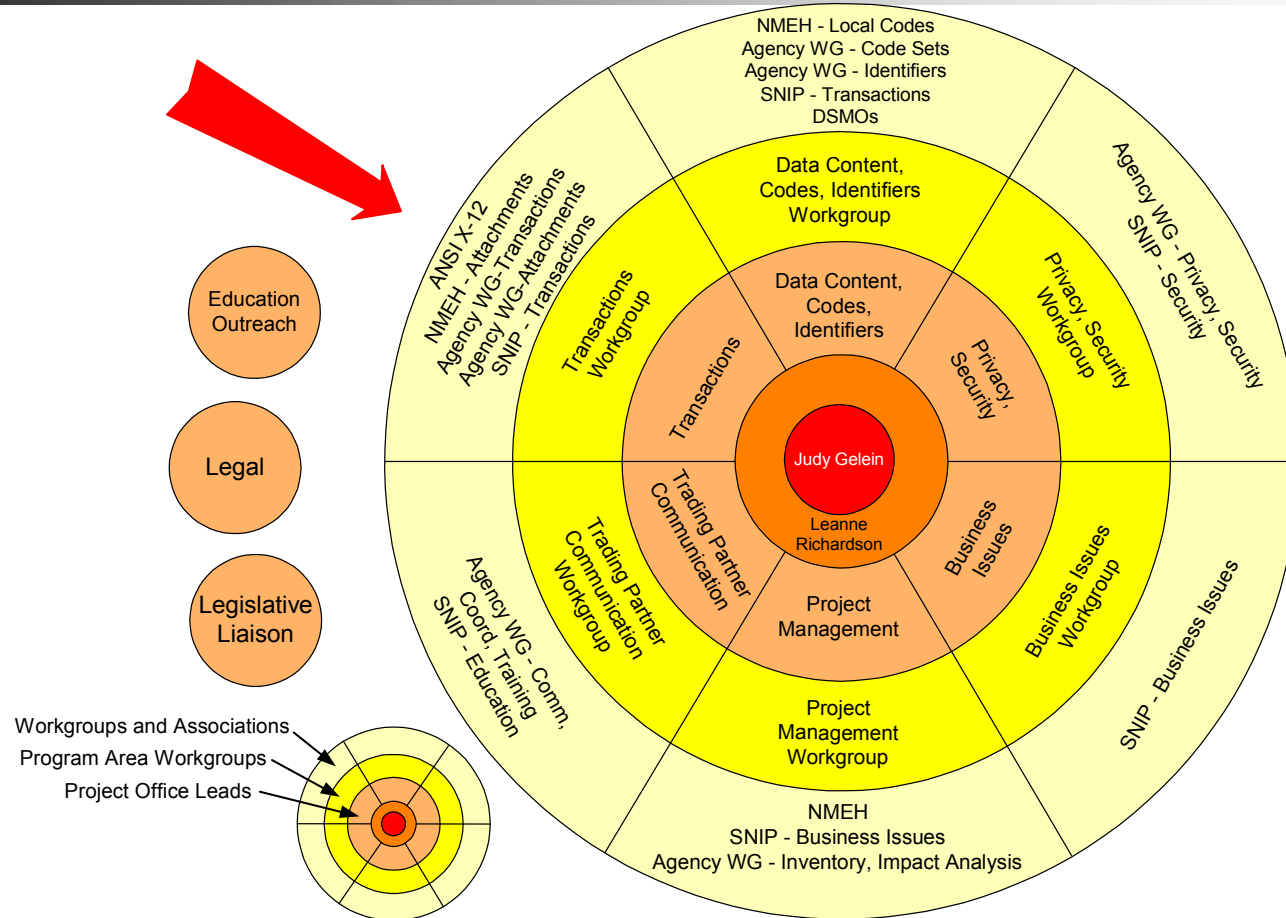
# Organization Structure for Implementation

---

- For some, a different organization is needed for Implementation vs Assessment
- For many, budget constraints call for a new approach
- Example from California



# Original California HIPAA Project Management Approach



# Project Planning Model

CA Department of Health Services

DHS HIPAA Compliance Program



Program Mgmt Plan

TCS Primary Project



Project Mgmt Plan

Privacy Primary Project



Project Mgmt Plan

Rule "N" Primary Project



Project Mgmt Plan

End-to-End Projects



Project Mgmt Plan

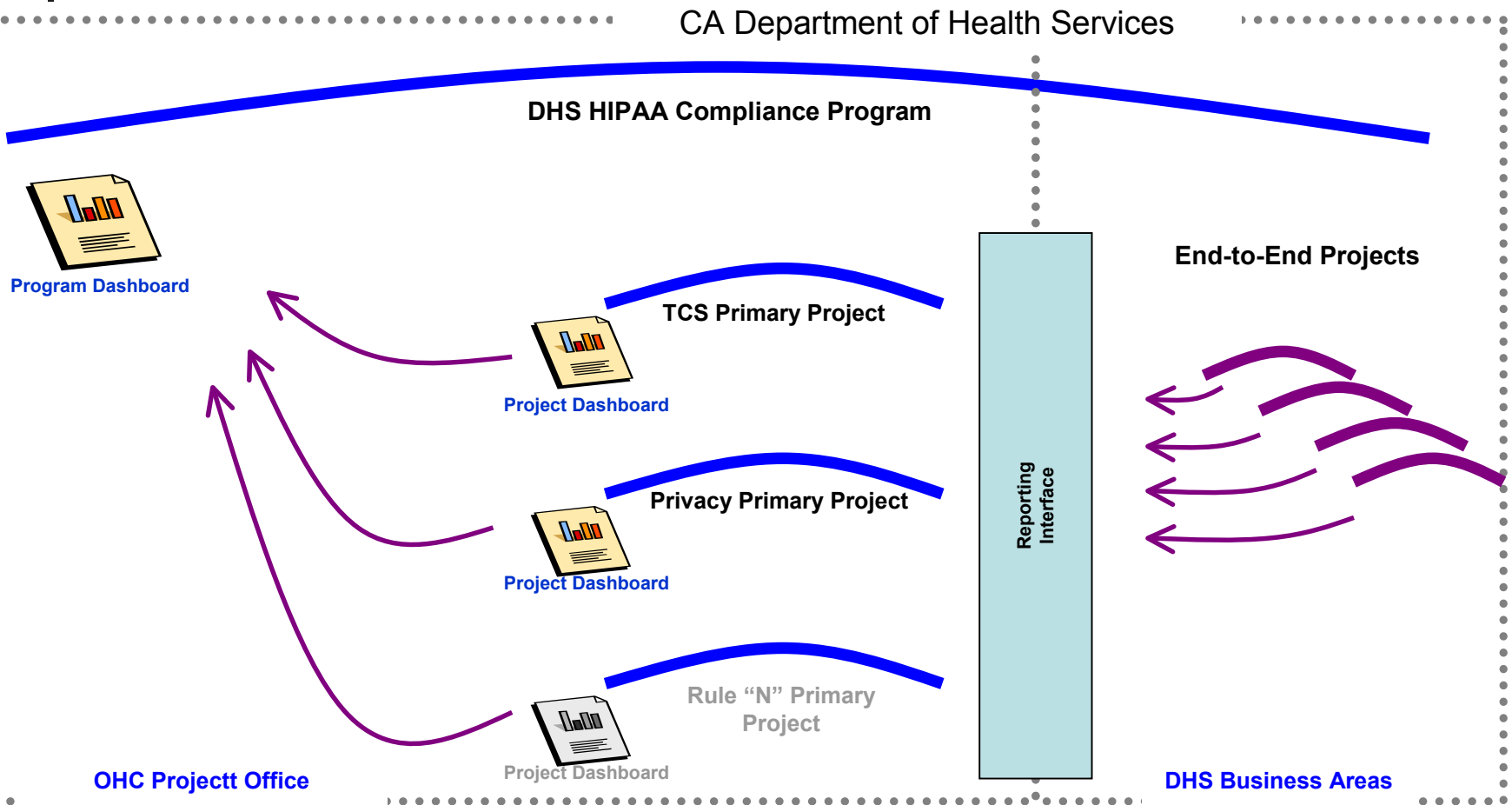


Project Mgmt Plan

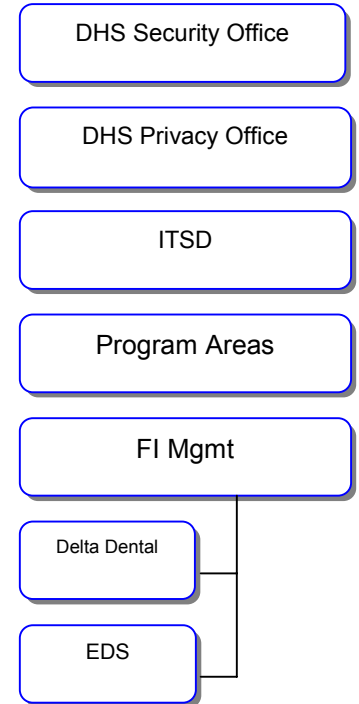
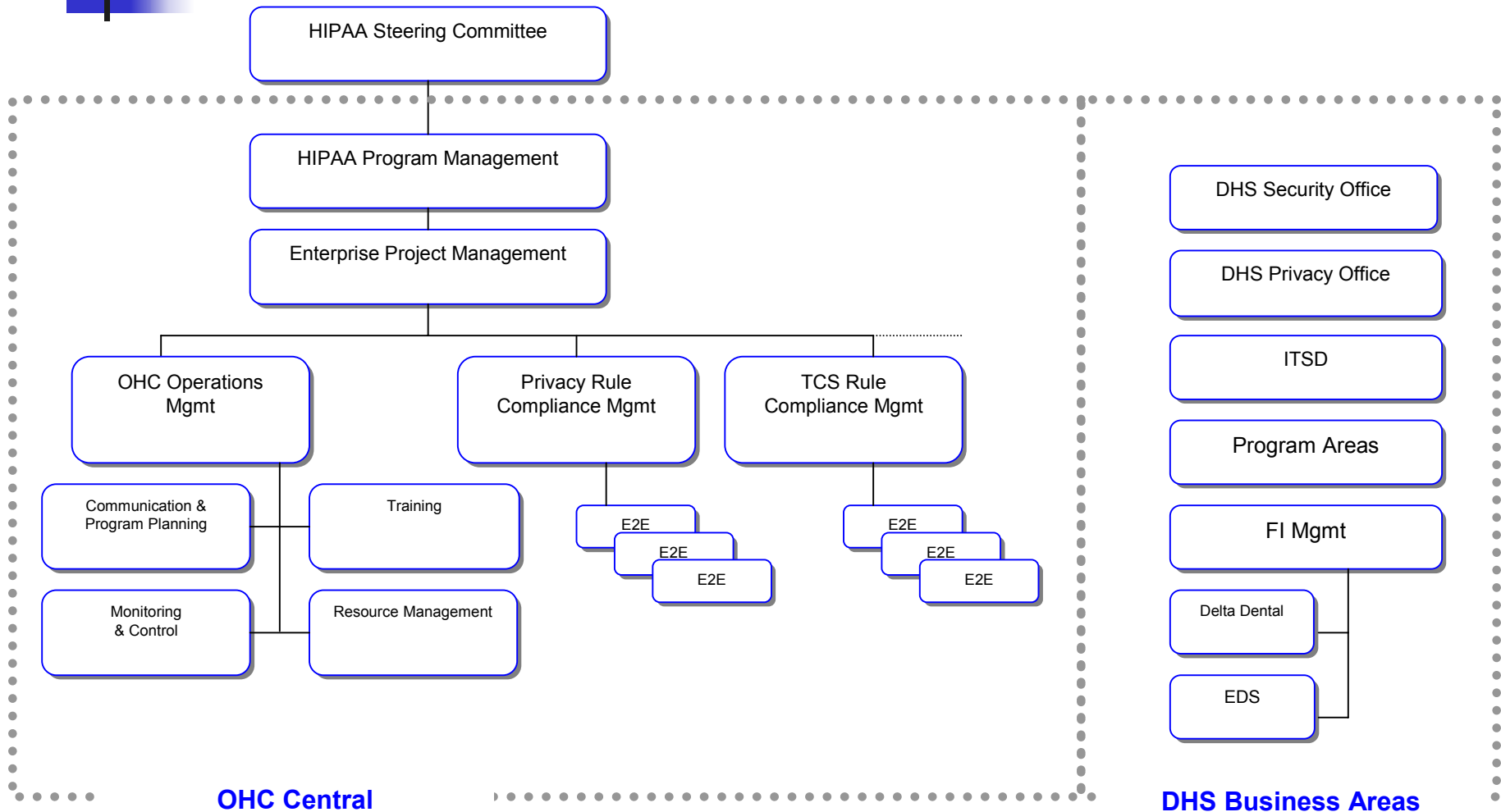
OHC Project Office

DHS Business Areas

# Project Monitoring & Control Model



# Conceptual OHC Organization





# READINESS PLAN AND SCHEDULE

---

*If You Don't Know Where You Are  
Going, Any Direction Will Do*



# Plan Description

---

- Portion of overall project plan
- Covers activities to demonstrate that systems and staff are ready to process HIPAA EDI
- Specifies each major activity
- Describes tasks, sequence, relationships, resources, schedule, and accountability
- It is NOT just an Information Systems plan



# Documenting Readiness

---

- Why Document?
  - HIPAA is a federal law
  - Justify funding and/or costs
  - Demonstrates due diligence
  - State law and federal regulations may conflict
- Risk
  - Critical to defending during litigation, complaints, and audits
  - It may be used against you
  - Mitigate risk: Establish guidelines and involve legal counsel to ensure appropriate documentation is maintained



# IDENTIFICATION OF READINESS ISSUES

---

*Are You "Waiting for Godot" or  
Can You Get on With the Show?*

Judy Gelein and Julie Dittman, State of California





# Definition of a Readiness Issue

---

- A Readiness Issue Is a HIPAA Implementation Problem That:
  - Jeopardizes compliance strategy
  - Significantly impedes progress on the project, and
  - Requires external responses or risk based decisions



# Examples of Readiness Issues

---

- Large number of requests for national codes to replace local codes
- Status of encounter data (require 837 or not; seeking DHHS direction)
- Determination of covered entity status, ambiguity between provider and health plan roles
- Local Code: no replacement, no workaround
- Information currently transmitted for MCO enrollment contains more data than the 834
- Inability to meet deadline for one or more transactions



# Strategy for Issue Resolution

---

- Document a strategy to resolve issues
- Determine when external issues become internal
- Meet deadlines for resolution
- Obtain external guidance
- Demonstrate due diligence
- Conduct a cost benefit, risk, or other analysis
- Inform trading partners



# TRADING PARTNER AGREEMENTS

---

*Are We All on the Same Page?*

Leah Hole-Curry, A-Team/ FOX Systems



# Trading Partner Agreement (TPA) – Description & Purpose

---

- Description

- Agreement between parties related to exchange of electronic transactions
- Establishes duties and common expectations between trading partners
- TPA cannot introduce additional or different non-standard data requirements
- Can be a basic agreement with an attached Billing Instruction

- Purpose - HIPAA transaction standards allow some payer discretion in situational fields or choice of data content. NOTE: IGs encourage development of TPAs



# Trading Partner Agreement Contents

---

- Connectivity and Testing requirements
- Acceptance/rejection criteria
- Transmission charges and who should pay
- Data clarifications where guides provide options
- Specification of:
  - Level of service
  - Current/interim security measures and requirements
  - Non-standard uses of standard transactions
  - Timing of processing cycles and responses to queries



# TESTING ZONES

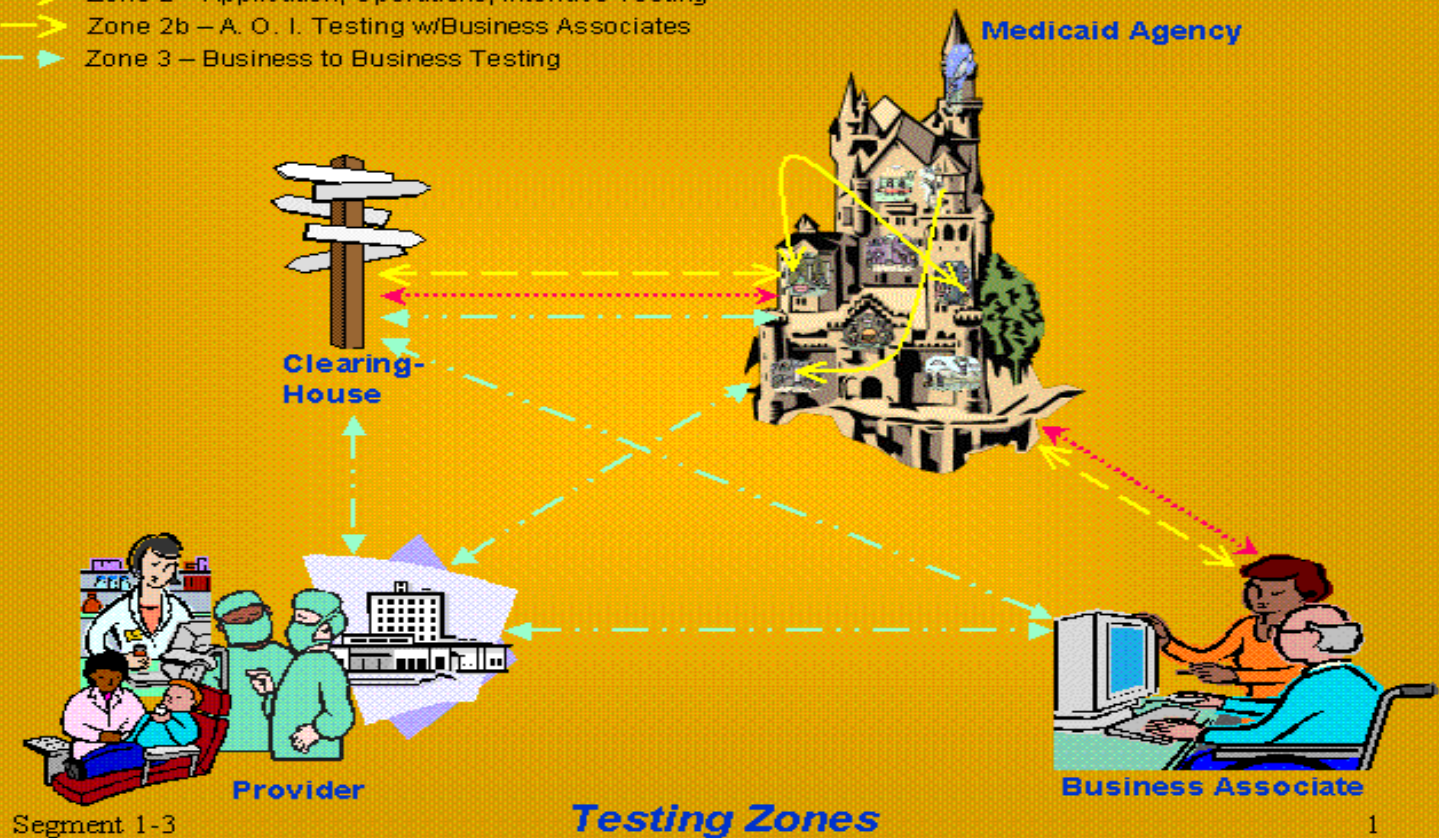
---

- Zone 1 - Compliance Testing
- Zone 2 Applications, Operations, and Interface Testing (Testing within the Medicaid Agency and with Business Associates)
- Zone 3 - Business-to-Business Testing

Susan Fox

# Testing Zones

- Zone 1 – Compliance Testing
- Zone 2 – Application, Operations, Interface Testing
- Zone 2b – A. O. I. Testing w/Business Associates
- Zone 3 – Business to Business Testing



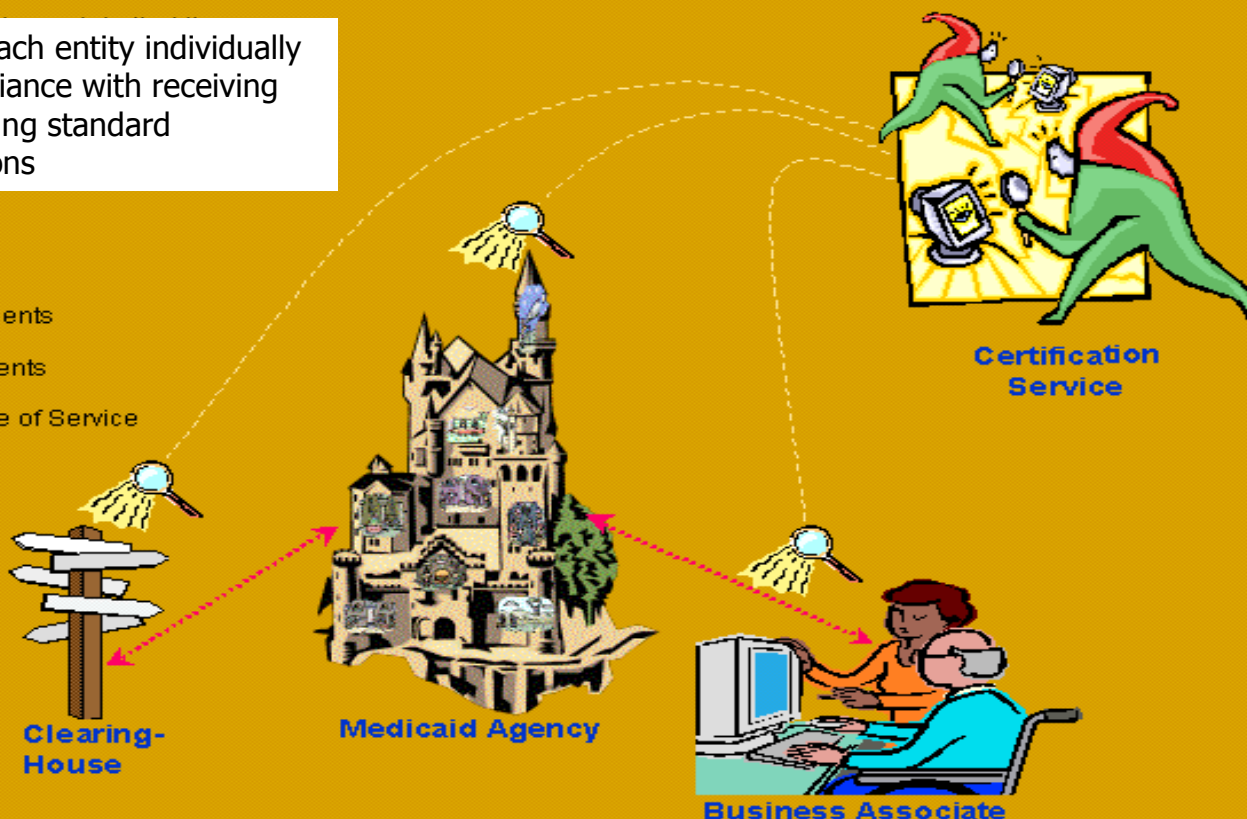


# Compliance Testing – Zone 1

Testing each entity individually for compliance with receiving and sending standard transactions

Includes Test Levels:

1. Transaction Integrity
2. HIPAA I.G. Requirements
3. Balancing
4. Situational Requirements
5. External Code Set
6. Product Types or Line of Service

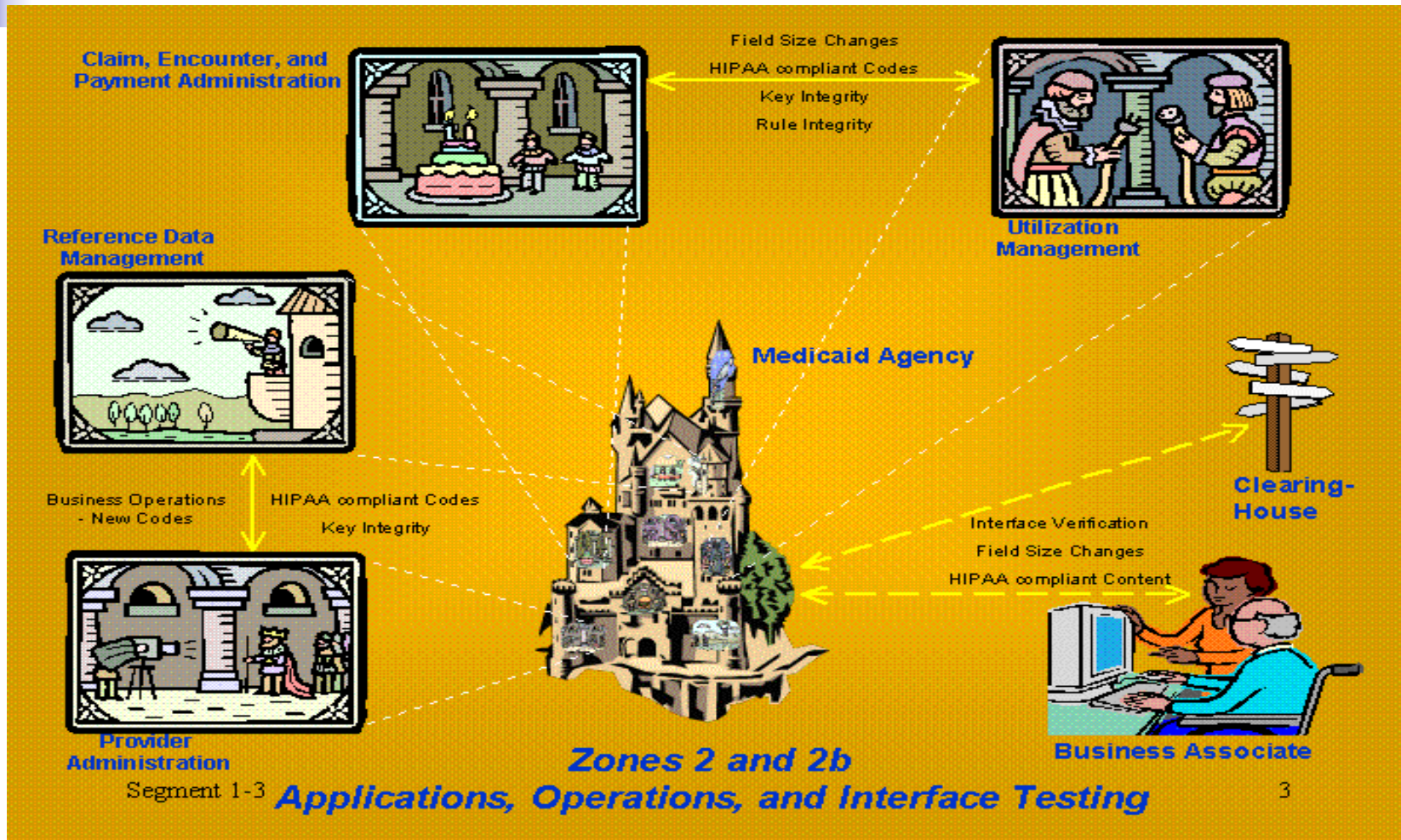


**Zone 1  
Compliance Testing**

Segment 1-3

2

# Applications, Operations, and Interface Testing – Zone 2

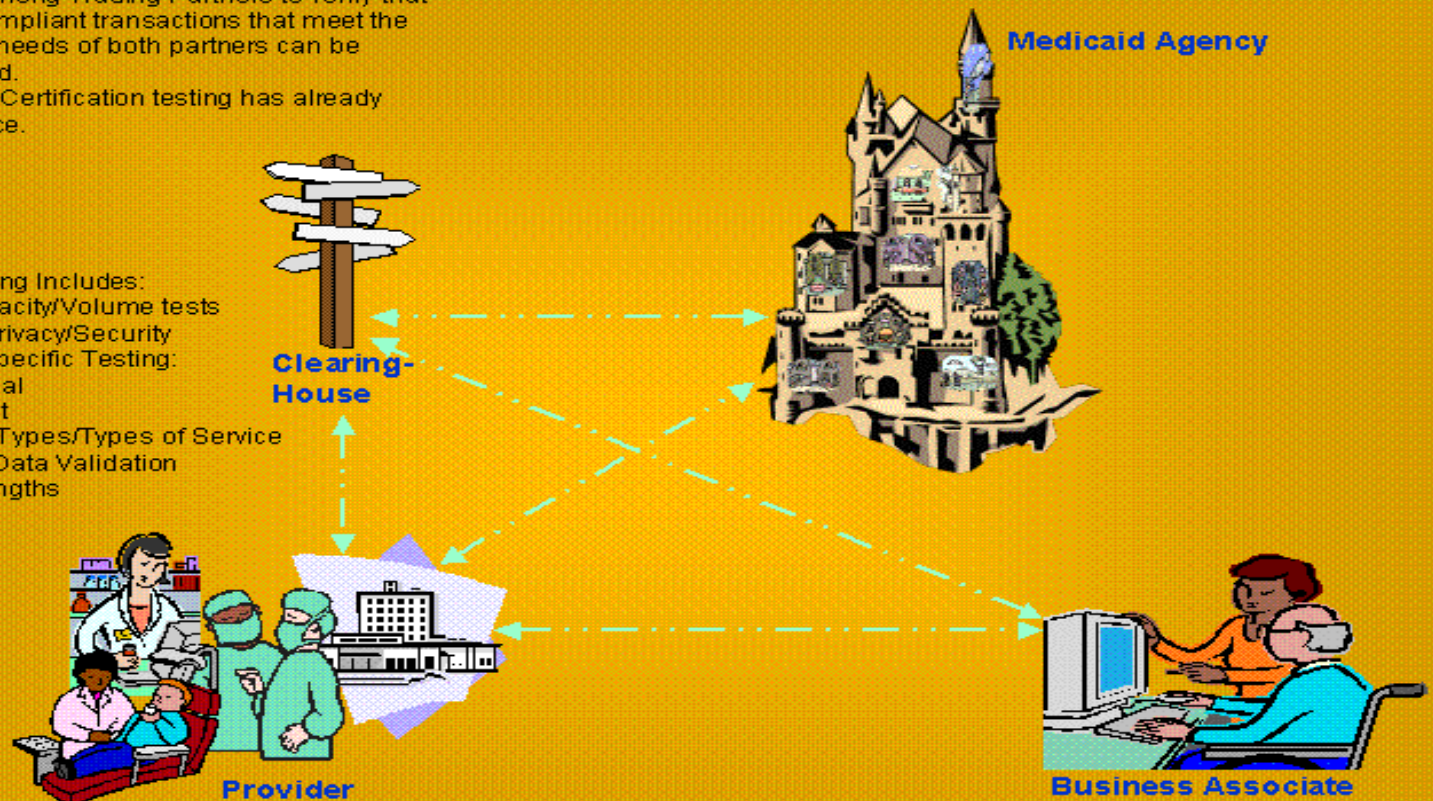




# Business to Business Testing – Zone 3

Testing among Trading Partners to verify that HIPAA compliant transactions that meet the business needs of both partners can be exchanged.  
Assumes Certification testing has already taken place.

This Testing Includes:  
Load/Capacity/Volume tests  
Verifies Privacy/Security  
Partner Specific Testing:  
Situational  
Code Set  
Product Types/Types of Service  
Partner Data Validation  
Field Lengths  
Output



Segment 1-3

**Zone 3**  
**Business to Business Testing**

4



# BUSINESS-TO-BUSINESS (B2B) TESTING

---

*Can We Talk?*

Peter Barry, Peter T. Barry Co.



# Description

---

- Structured test between payer and data trading partners, post compliance certification
- Ensures that partners' in-bound transactions can be received, validated, and processed
- Ensures that partners can receive out-bound transaction
- Note: Some payers believe that compliance certification is all that is needed



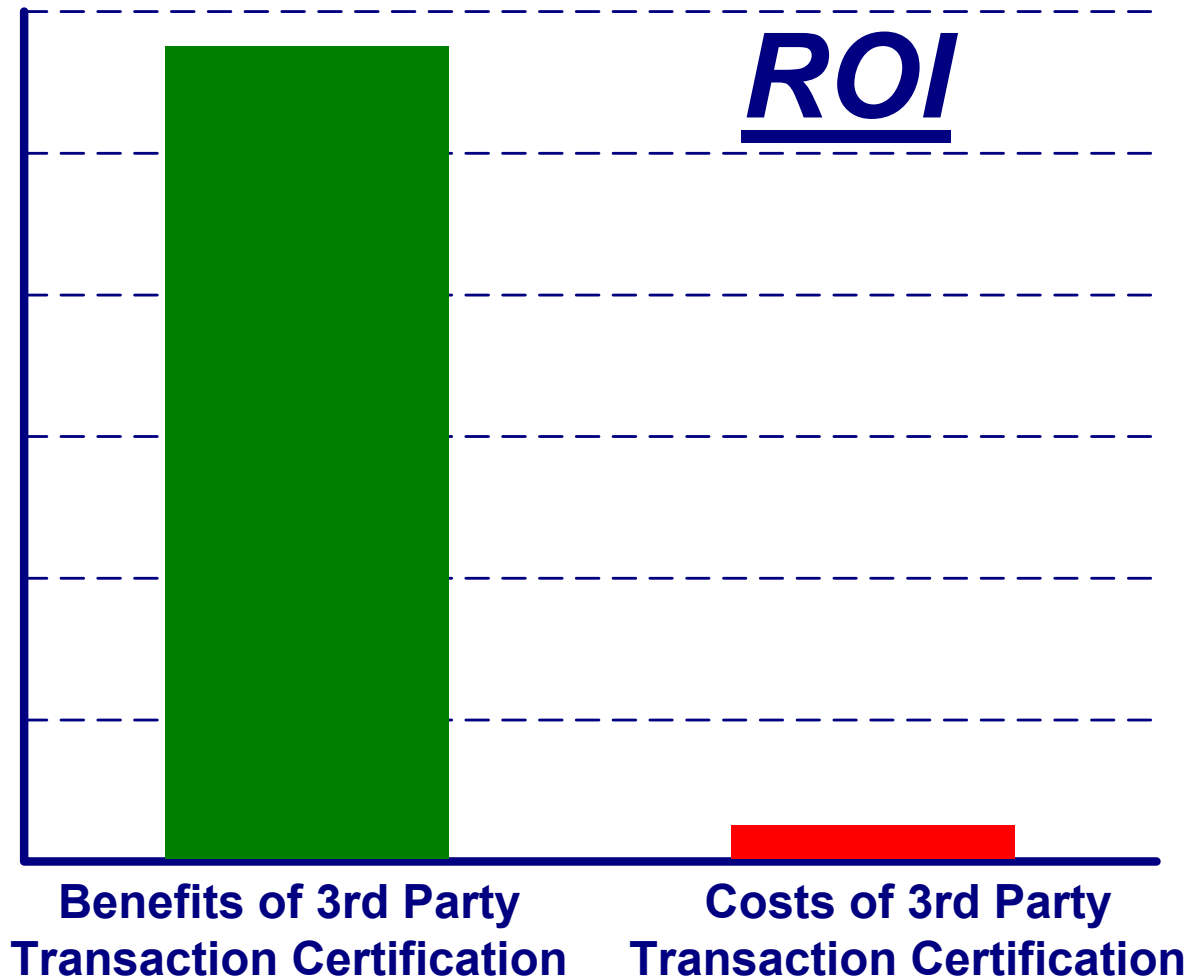
# COMPLIANCE TESTING

---

*Making Sure Our Language is Pure*

Peter Barry, Peter T Barry Company

# TRANSACTION TESTING AND CERTIFICATION





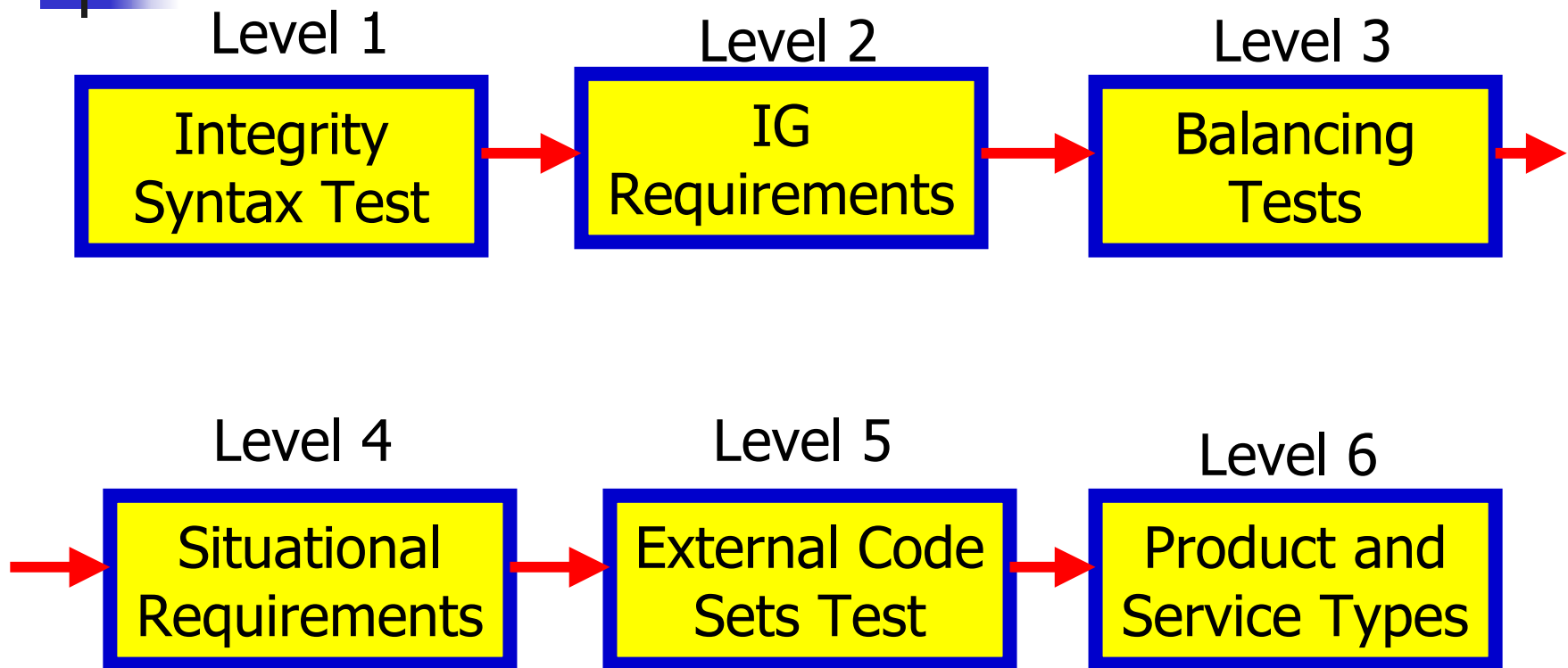
# Testing Alternatives

---

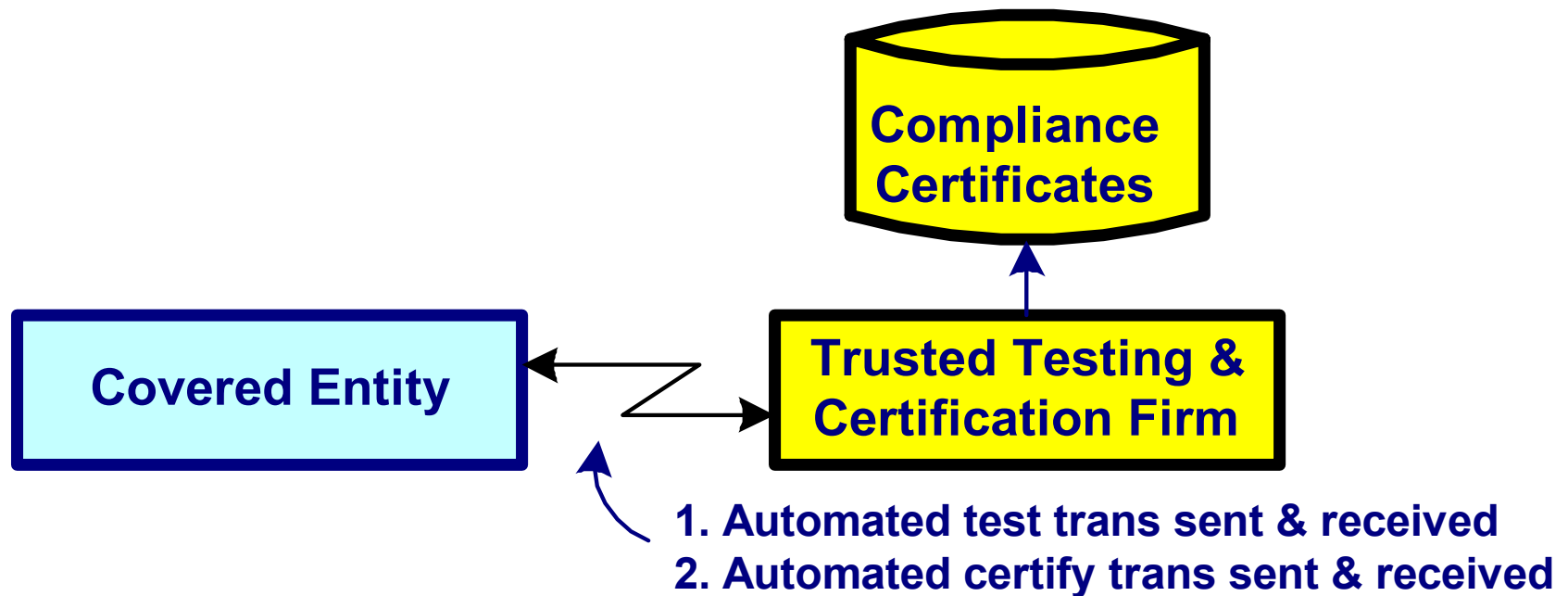
- Do it yourself. Test own systems in-house, then test one-on-one with partners.
- Contract to test your systems, then test one-on-one with partners
- Use trusted third-party certification.
  - Test own systems against the middle
  - Partners test their systems against the middle
  - Then go one-on-one, ready for production.



# SNIP 6 Levels of Compliance Testing



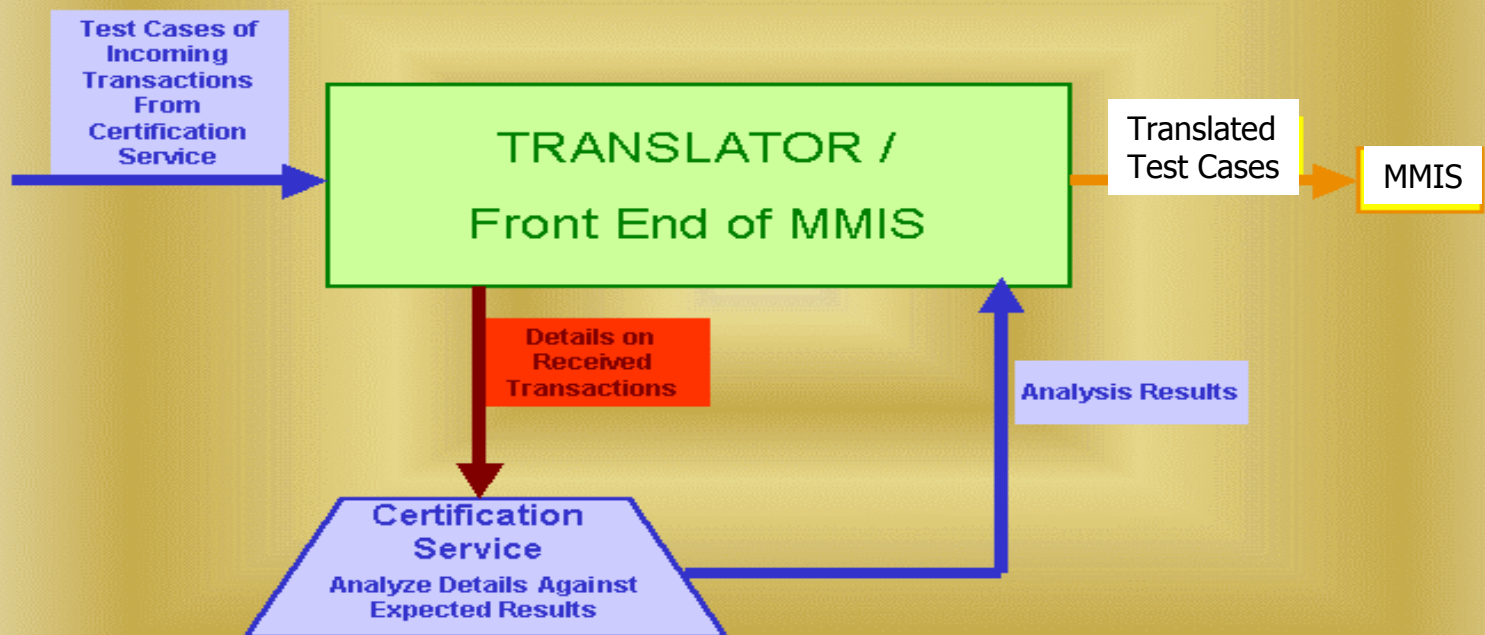
# What is Third-Party Transaction Certification?



## Third-party Transaction Certification

# Certification Service Inbound Test

## Testing Incoming Transactions with Test Cases from a Certification Service





# The Transaction Certification Process

---

- Get your systems ready to test.
- Test your system with Trusted 3rd Party.
- Certify with the Trusted 3rd Party.

Note 1: Certificate should include detailed list of the capabilities you have demonstrated.

Note 2: It is just as important to certify ability to receive standard transactions.

# Why Certify?

1.7

## Why not just Test?

---

- No more work, no added cost to certify after completion of complete testing.
- Certification assures objective compliance
- Within entity, certification is the standard of performance, the passing grade.
- With trading partners, certification is good faith demonstration of readiness.
- For industry, reduces risk of cash flow disruption, increases confidence.



# Definition of Certified Entity

## Single Source of Error Principle

---

*Definition:* A **Certified Entity** is workflow of payer, provider, clearinghouse, vendor, or system that embodies only a **single source of error**.

- If two systems, certify two entities.
- Clearinghouse certifies self and all clients.
- Vendor certifies self and all installations.
- Billing service certifies its clients.



# You should require trading partners to certify.

---

- It is not legally mandated and it would be unreasonable and unfair to burden one party, who has exhaustively tested and certified its own capability, to run debug tests one-on-one with trading partners who have not yet made their systems compliant.
- It is entirely reasonable, as a condition of doing business, to require trading partners to certify.



# Benefits of Third-Party Certification

---

- Savings: (1) own system, (2) trading partners
- Enables industry to meet the deadline
- Avoids last minute chaos of the deadline
- Significant reduction of risk and liability
- Certify at your own pace, don't wait for others
- Much, much faster
- Everyone measures against same standard
- Avoid disputes between trading partners





# Benefits of Third-Party Certification

---

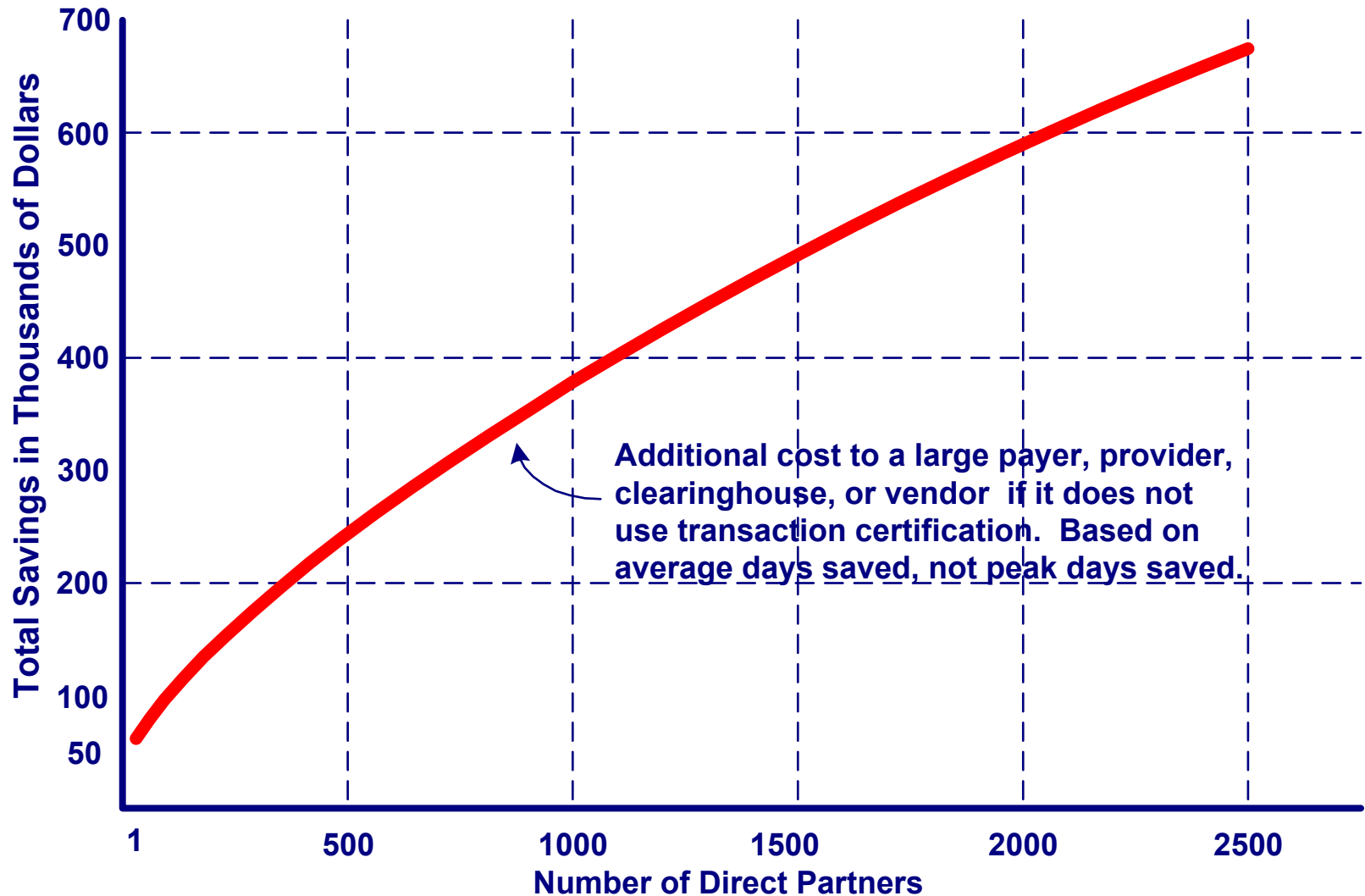
- Avoid contract disputes
- Demonstrate good faith effort, could be critical in defending liability
- Certification list exact capabilities
- Reduction in production errors
- Purchasers can independently determine if vendor or business associate complies
- Requires only one-third average support staff and only one-fourth peak staff.



# Savings for Large Entity

Method	Testing Own System	Plus Per Trading Partner
<b>Do it yourself, 1:1 testing</b>	230 person-days \$92,000 cost	12-15 hours \$375 / partner
<b>Third-party Certification</b>	67 person-days \$32,800 cost	2-4 hours \$125 / partner
<b>Savings</b>	163 person-days \$60,000	8 hours \$250 / partner

# Total Savings Large Entity





# Transaction Certification is Only Way to Meet Deadline

Estimate for Large Payer or Clearinghouse 2500 Partners

<b>Large Entity 2500 Partners</b>	<b>Average Staff</b>	<b>Peak Demand Factor</b>	<b>Peak Staff</b>
<b>Without Certification</b>	30 Persons	2.00	60 Persons
<b>With Certification</b>	10 Persons	1.50	15 Persons



## Savings by Type of Entity

Type of Entity	Savings
Large Payer or Clearinghouse with 2500 Partners	\$680,000
Hospital with Own System 150 Partners	\$106,000
Large Vendor	\$60,000 plus \$2,000 per site
Small Provider	\$2,000+ implicit in upgrade or fees

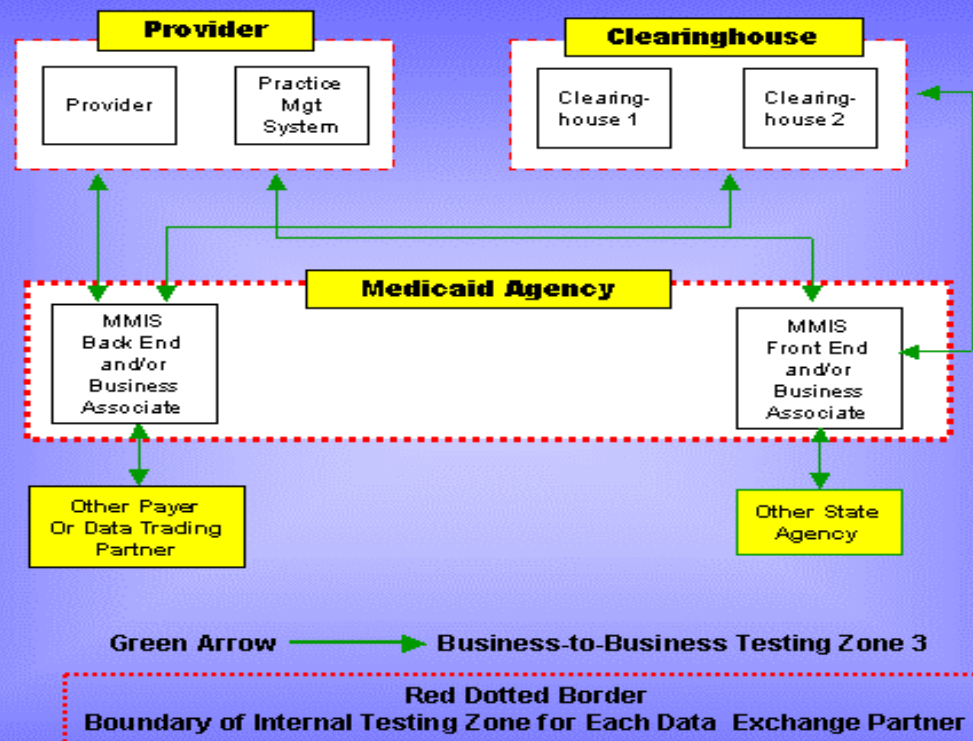


# Summary of Certification

---

- Large savings in cost and time.
- All entities, large and small, can and should require certification of partners.
- Certification will help you meet deadline.
- So Certification is a Total Win-Win.
- Recommendation:
  - Certify your own capabilities.
  - Require certification from trading partners.

# B2B Testing Partners





# Guidelines

---

- Both payer and provider should be certified for compliance in sending/receiving
- State may limit B2B testing to high volume, critical providers only
- Test with as many of your provider types as possible, e.g., M.D., Ambulance, etc.
- Test at a minimum the most critical transactions
- State may require that providers have external entity certify compliance first





## Guidelines (2)

---

- Establish criteria to allow a provider to test
- Establish criteria and success rate (% of tests passed) for completion of B2B test phase
- Inform partners who pass test and send Trading Partner Agreement information
- Track compliant partners
- Train help desk staff to resolve problems with partners' tests (before, during & after)



# Recommendations

---

- Use WEDI/SNIP guidelines for B2B testing
- Use regional SNIP guidelines
- Consider combining B2B testing with applications and interface testing to complete an End-to-End test



# APPLICATIONS, OPERATIONS, AND INTERFACE TESTING

---

*Your Old Friend —  
With a Few New Habits*

Mark Charles, State of Michigan



# What Needs To Be Tested - Applications

---

## Front-end Edits and New Conversion Routines

- Front-end edits not handled by translator; edits to weed out “HIPAA nonsense”
- Logic to build data elements that are no longer carried on the claim and are not part of the translator functions
- Conversion routines to process information entering the MMIS via routes other than EDI



# What Needs To Be Tested – Applications (2)

---

## All Other Application Functions

- Incoming information – edits and associated logic to process system inputs through adjudication, prior authorization, etc.
- Maintenance and management – e.g., reference files, history files
- Outgoing information – production of system outputs, including derived values and retrieval of stored values (previously stripped)



# What Needs to be Tested – Operations and Interfaces

---

- Re-engineered, newly developed (including work-arounds), and all manual business processes
- Staff's ability to work with HIPAA compliant data, especially new standard codes
- External interfaces with other agencies, other payers, other trading partners
- Internal interfaces with all business associates, e.g., FA, enrollment broker, prior auth agent, and other independent systems within the enterprise



# Testing Methodology

---

- Current testing procedures can be used as baseline
- Initiate test team(s) early in development
- Additional incremental/iterative testing may be necessary due to complexity of HIPAA
- Thorough testing includes end-to-end tests
- System areas more heavily impacted by HIPAA will require more intensive testing
- Develop test data in increments by transaction, by provider type, by portion of the MMIS (subsystem, interface)
- Develop Business Scenarios to test HIPAA transactions, lines of business, complex business rules, etc.



# TRANSITION PLAN AND SCHEDULE

---

*It All Works,  
Now Let's Get It in Use!*

Susan Fox





# Plan Description

---

- Defines the sequence and schedule for the phase-in of all transactions for all provider types
- Depicts the migration of providers from current processes to the new HIPAA standards
- Shows the cut-over date after which pre-HIPAA path is discontinued

# TRANSACTION SEQUENCING PLAN



---

*Who's On First?*

Susan Fox



# Sequencing Plan Description

---

- Sequence and schedule for the phase-in of each transaction or set
- Start date for accepting new transaction (on or before deadline)
- Cut-over date (date after which prior format will be rejected)
- Separate transition dates for provider types
- Separate transition dates for data submission type: EDI, DDE, Web, Paper

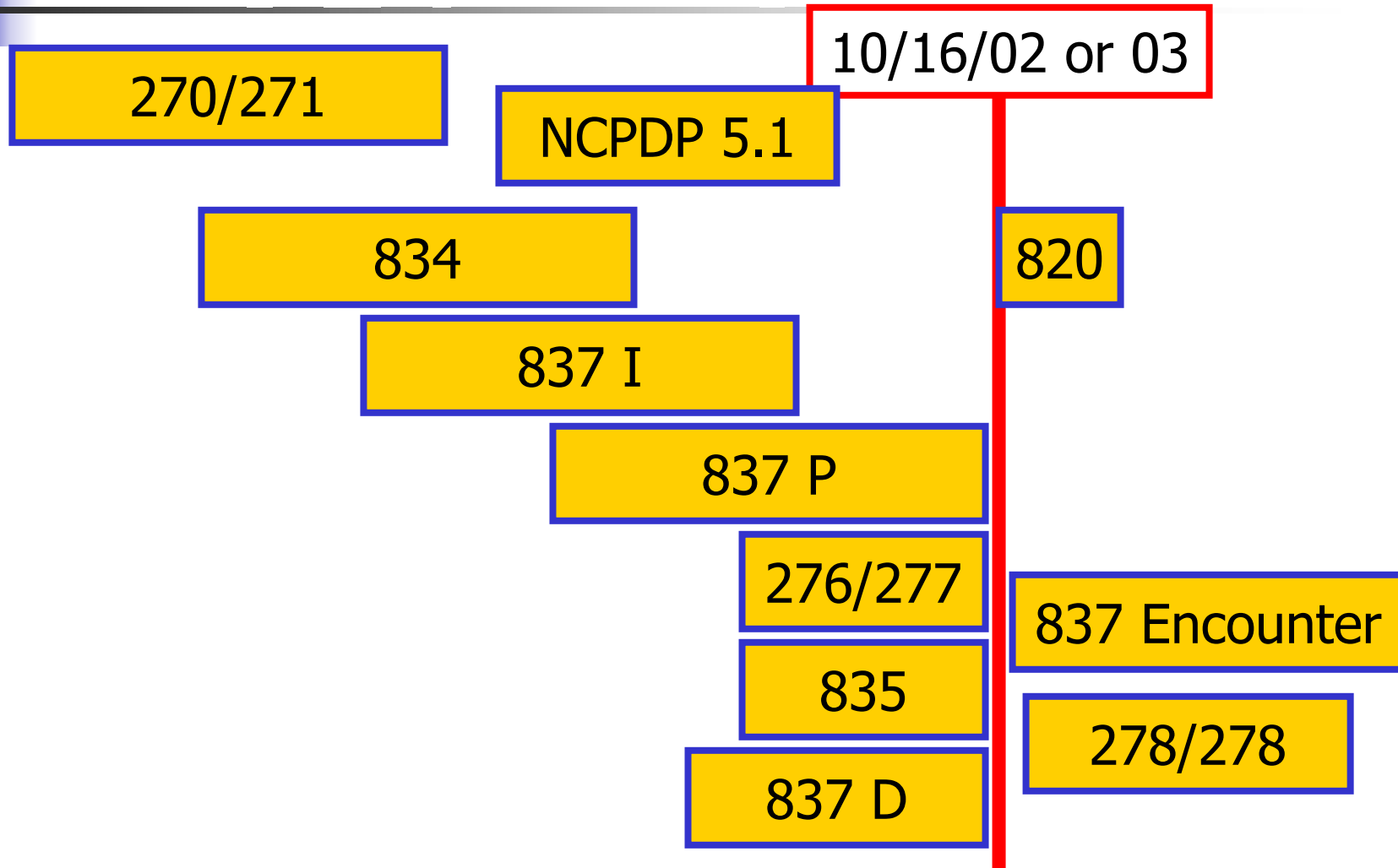
# Example of Phase-in Plan per WEDi/SNIP (Adapted)

**Schedule and Sequence Implementation Proposal \*\***

	<b>Group 1</b>	<b>Group 2</b>	<b>Group 3</b>	<b>Group 4</b>	<b>Group 5</b>
<b>Transaction Groups</b>	837 835	270/271 834	276/277	278	820
<b>Pilot/Testing Period</b>	Jul 1, 2002	Nov 1, 2002	Feb 1, 2003	Mar 1, 2003	April 1, 2003
<b>Payer Readiness Date</b>	Oct 2002 14 <sup>th</sup> month	Mar 1, 2003 19 <sup>th</sup> month	May 2003 21 <sup>st</sup> month	June 2003 22 <sup>nd</sup> month	Aug 2003 24 <sup>th</sup> month
<b>Final Implementation</b>	Oct 17, 2003	Oct 17, 2003	Oct 17, 2003	Oct 17, 2003	Oct 17, 2003

\*\*This chart is shown only as an illustration of a logical grouping of transactions. The original WEDi/SNIP dates are shown updated by one year to illustrate potential schedule for an entity that has filed for the extension. The date for Pilot/Testing Period has been changed from May to April to conform with the requirement of the law that testing must begin by April, 2003.

# Example of Phase-in Plan





# Sequencing Considerations and Operations Start Dates

---

- Criteria for determining sequence of transactions
- Possible criteria for determining sequence of provider types
- Factors to consider when determining the operations start date of each transaction



# TRANSITION ISSUES

---

*The Time Before...*  
*The Time After Cut-Over...*  
*And The Space In Between*

Susan Fox



# Transition Issue Description

---

- A transition issue occurs when a business process is supported by data that may be required to be in two different formats
  - Transactions and files that may be subject to two sets of requirements for format and content
  - Transaction pairs that straddle the compliance date



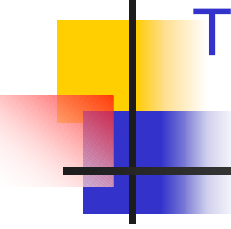


# Transition Issues Examples

---

- Date of service determines data content, date of transmission determines EDI format
- Some transactions come in pairs
- Some transactions are dependent on others
- Files, both Reference and History, used after transition must support both standard and non-standard code sets and/or differing sets of information
- Reporting that covers dates straddling the transition start date must process data in both standard and non-standard formats

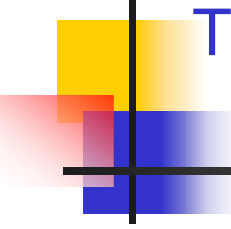
# Twisted Sisters: Transaction Pairs That Straddle the Compliance Date Line



NON-STANDARD EDI TRANSACTIONS PRIOR TO COMPLIANCE DEADLINE	OCT 16**	STANDARD TRANSACTIONS AFTER DEADLINE
NON-STANDARD CLAIM SUBMITTED		ELECTRONIC RA (835)
NON-STANDARD CLAIM SUBMITTED		
CLAIM STATUS REQUEST		CLAIM STATUS RESPONSE
SERVICE PROVIDED		EDI CLAIM SUBMITTED
CLAIM STATUS REQUEST SENT		CLAIM STATUS RESPONSE
CLAIM SUBMITTED		SUPPLEMENTAL CLAIM SUBMITTED

**\*\*October 16, 2002 or 2003 or any earlier date the entities agree on for implementation**

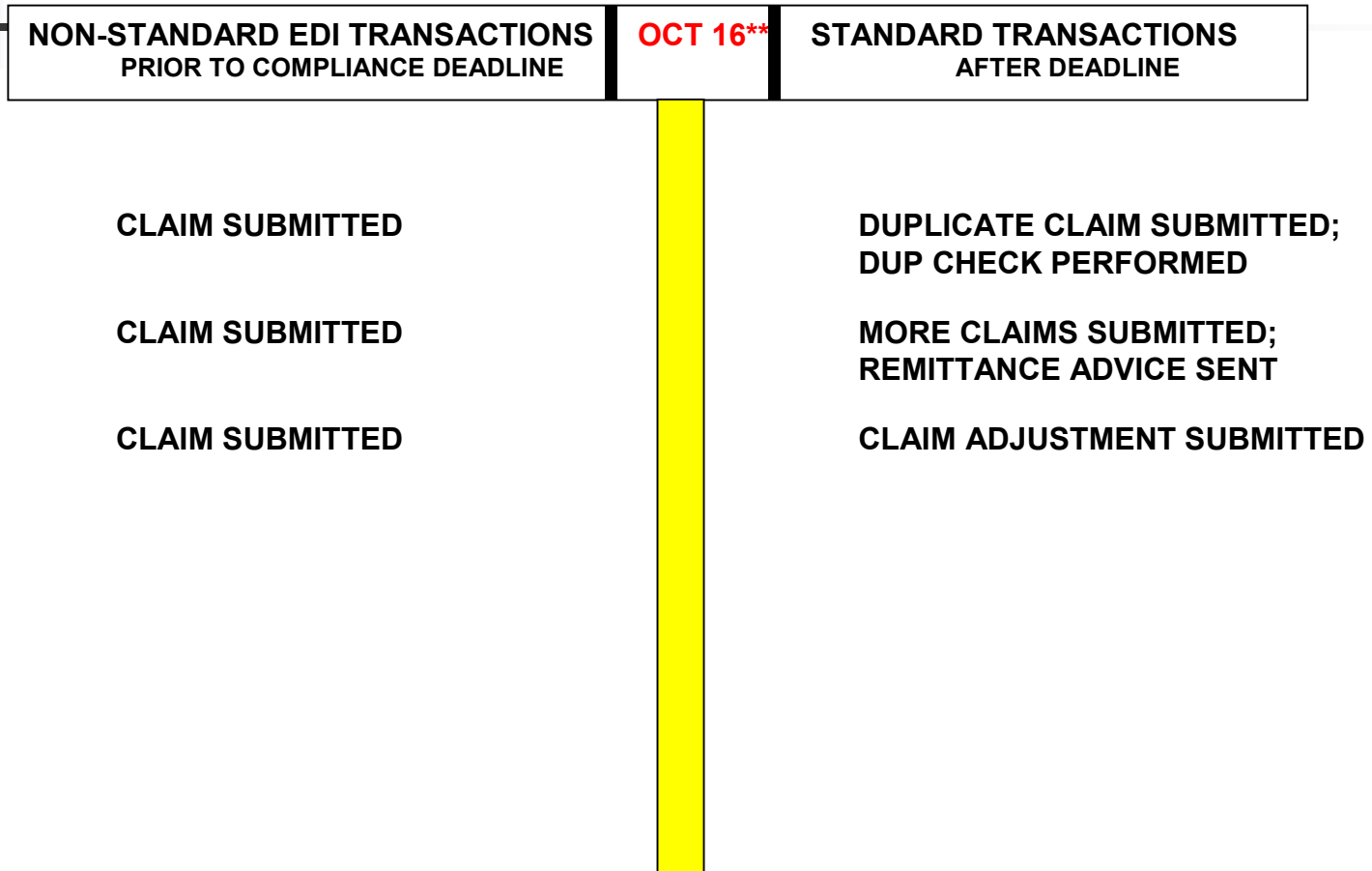
# Twisted Sisters: Transaction Pairs That Straddle the Compliance Date Line



NON-STANDARD EDI TRANSACTIONS PRIOR TO COMPLIANCE DEADLINE	OCT 16**	STANDARD TRANSACTIONS AFTER DEADLINE
ENCOUNTER SERVICE PROVIDED		ENCOUNTER SUBMITTED
BATCH EVS REQUEST		ELIGIBILITY RESPONSE
PRIOR AUTHORIZATION REQUEST		PA RESPONSE
ENROLLMENT TRANSMITTED		DISENROLLMENT/CHANGES
CLAIM RECEIVED		RESPONSE TO REQUEST
MORE INFORMATION REQUESTED		

**\*\*October 16, 2002 or 2003 or any earlier date the entities agree on for implementation**

# Twisted Sisters: Transaction Pairs That Straddle the Compliance Date Line



**\*\*October 16, 2002 or 2003 or any earlier date the entities agree on for implementation**



# TRANSITION: OPERATIONS & MONITORING

---

*All Roads Lead to Rome*



# Begin Parallel Operations

---

After validating that the parallel environment is ready:

- Notify all affected parties
- Ensure trading partner readiness
- Process HIPAA compliant claims
- Begin monitoring phase
- Verify effectiveness of business process training



# Monitoring The Transition

---

- Monitor problems – meter TPs onto system, track problems including those reported by TPs
- Monitor trading partners migration- establish criteria for permanent migration or to move a TP who is not ready, back to the current system
- Monitor workload moved – monitor percentage of workload on new system to achieve a desired rate of transfer, rate of increase must meet schedule
- Monitor system capacity use – HIPAA system has new functions, efficiency of software not known, ensure that system can handle projected HIPPA workload



# Conclusions

---

- Overall planning and scheduling is necessary to ensure a smooth transition
- Following the plan is necessary to achieve compliance
- Documenting the decisions, processes, and results is important to be able to substantiate and provide proof of due diligence